

(19)日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-278931

(P2002-278931A)

(43)公開日 平成14年9月27日(2002.9.27)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 B 0 1 7
	3 1 0		3 1 0 D 5 B 0 8 5
12/14	3 2 0	12/14	3 2 0 F
13/00	5 1 0	13/00	5 1 0 S
17/60	3 1 4	17/60	3 1 4

審査請求 有 請求項の数14 O L (全 9 頁)

(21)出願番号 特願2001-81479(P2001-81479)

(22)出願日 平成13年3月21日(2001.3.21)

(71)出願人 397011373

ソニーコミュニケーションネットワーク株式会社

東京都品川区北品川4丁目7番35号

(72)発明者 森田 巧

東京都品川区北品川4丁目7番35号 ソニーコミュニケーションネットワーク株式会社 社内

(74)代理人 100105924

弁理士 森下 賢樹

Fターム(参考) 5B017 AA03 BA05 BA07 BB10

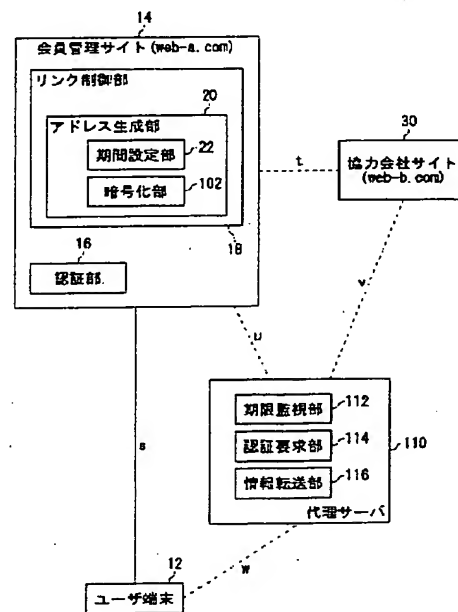
5B085 AA08 AE02 AE03 AE29 BA06  
BC01

(54)【発明の名称】 ログイン管理方法およびシステム

## (57)【要約】

【課題】 複数のサイトが協力関係をもっても、それぞれがユーザを認証すればユーザの利便性が悪く、サービスの一体感に欠ける。

【解決手段】 第1のサイトである会員管理サイト14は、第2のサイトである協力会社サイト30へのリンクを提供する。アドレス生成部20は、ユーザがリンク箇所をクリックしたとき代理サーバ110のURLをユーザ端末12へ設定する。この際、サービスに時間制限を設ける。代理サーバ110は自ら協力会社サイト30へログインし、情報をユーザ端末12へ転送する。



## 【特許請求の範囲】

【請求項1】 ユーザが認証のための情報を入力してネットワーク上の第1のサイトへログインした後、そのサイトからリンクを辿って第2のサイトへのログインを試みたとき、第1のサイトに前記認証のための情報を第2のサイトへアクセスするためのアドレスに付加して当該アクセスに提供することを特徴とするログイン管理方法。

【請求項2】 前記認証のための情報の有効期限を第1のサイトから第2のサイトへ適宜設定し、第2のサイトは第1のサイトからリンクを辿ってログインするユーザのアクセスを前記有効期限内に限り許可することを特徴とする請求項1に記載の方法。

【請求項3】 ユーザが所定のサイトへのログインを試みたとき、そのユーザをそのサイトを代理する中継拠点へ導く工程と、

その中継拠点にて得られた前記サイトの情報をその中継拠点からユーザへ提供する工程とを含み、前記中継拠点が前記サイトの情報を得る際、そのサイトに認証のための情報を送信し、そのサイトからひとりのユーザとして認証された後、そのサイトへログインすることを特徴するログイン管理方法。

【請求項4】 ユーザが認証のための情報を入力してネットワーク上の第1のサイトへログインした後、そのサイトからリンクを辿って第2のサイトへのログインを試みたとき、そのユーザを第2のサイトの代理サーバへ導く工程と、

その代理サーバにて得られた第2のサイトの情報をその代理サーバからユーザへ提供する工程とを含み、前記代理サーバが第2のサイトの情報を得る際、第2のサイトからひとりのユーザとして認証された後、第2のサイトへログインすることを特徴するログイン管理方法。

【請求項5】 前記ユーザが前記リンクを辿る際、第1のサイトはそのユーザが第2のサイトの情報を得ることができる有効期限に関する情報を前記代理サーバへアクセスするためのアドレスへ付加して当該アクセスへ提供することを特徴とする請求項4に記載の方法。

【請求項6】 前記有効期限に関する情報は暗号化されており、前記代理サーバはその情報を復号して解釈し、その有効期限が切れたときそのユーザに対する第2のサイトの情報の提供を停止することを特徴とする請求項5に記載の方法。

【請求項7】 第1のサイトを含むログイン管理システムであって、

前記第1のサイトは、ユーザが認証のための情報を入力してログインを求めたときユーザを認証する認証部と、ログインしたユーザに対して第2のサイトへのリンクを提供するリンク制御部とを含み、

前記リンク制御部は、前記認証のための情報を付加した

形で前記ユーザが第2のサイトへアクセスするためのアドレスを生成するアドレス生成部を含むことを特徴とするログイン管理システム。

【請求項8】 前記第1のサイトはさらに、前記認証のための情報の有効期限を第2のサイトへ適宜設定する期限設定部を含むことを特徴とする請求項7に記載のシステム。

【請求項9】 ユーザが所定のサイトへアクセスする際、そのアクセスを仲介する中継拠点を含むログイン管理システムであって、

前記中継拠点は、

前記サイトから、自身がユーザとして認証を受けるために必要な情報を送信する認証要求部と、

前記サイトからユーザとして認証されたとき、このサイトへログインして取得した情報を前記ユーザへ提供する情報転送部と、

を含むことを特徴するログイン管理システム。

【請求項10】 第1のサイトと代理サーバを含むログイン管理システムであって、

前記第1のサイトは、ユーザが認証のための情報を入力してログインを求めたときユーザを認証する認証部と、ログインしたユーザに対して第2のサイトへのリンクを提供するリンク制御部とを含み、

前記リンク制御部は、前記ユーザが前記代理サーバへアクセスするためのアドレスを生成するアドレス生成部を含み、

前記代理サーバは、第2のサイトから、自身がユーザとして認証を受けるために必要な情報を送信する認証要求部と、第2のサイトからユーザとして認証されたとき、このサイトへログインして取得した情報を前記ユーザへ提供する情報転送部とを含むことを特徴するログイン管理システム。

【請求項11】 前記アドレス生成部は、前記ユーザが第2のサイトの情報を得ることができる有効期限に関する情報を前記アドレスへ付加することを特徴とする請求項10に記載のシステム。

【請求項12】 前記アドレス生成部は、前記有効期限に関する情報を暗号化したうえで前記アドレスへ付加することを特徴とする請求項11に記載のシステム。

【請求項13】 前記代理サーバはさらに、前記有効期限に関する情報を解釈してその期限の経過を監視する期限監視部を含み、その期限が経過したとき前記ユーザへの情報の提供が停止されることを特徴とする請求項11、12のいずれかに記載のシステム。

【請求項14】 ユーザが最初にログインする第1のサイトと代理サーバとを含むログイン管理システムであって、

前記代理サーバは前記第1のサイトと類似するドメイン名のもとで構築され、

ユーザが第1のサイトとセッションを有している間に第

2のサイトへのログインを要求したとき、前記第1のサイトはそのユーザのアクセス先を前記代理サーバへ変更し、

前記代理サーバは、そのユーザに代わって第2のサイトから情報を取得してこれをそのユーザへ提供することを特徴とするログイン管理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、ログイン管理技術に関し、とくに、ユーザがネットワーク上のあるサイトへログインするとき、これを制御するログイン管理方法およびシステムに関する。

【0002】

【従来の技術】ネットワーク、とくにインターネットを利用した電子商取引は、近い将来国家経済の大きな割合を占める勢いである。いわゆるIT関連企業は当然としても、従来ITとは無縁だった企業も、ウェブサイトを構築して情報を発信する姿勢が生き残りのための必要条件に思える状況である。

【0003】こうした状況下、ASP (Application Service Provider) ビジネスが拡大している。企業は最適なウェブサイトの設計、構築、および運用の一部または全部をASPに委託し、インターネットを通じたビジネスの拡張をアウトソーシングによって迅速かつ効率的に展開しつつ、既存ビジネスの安定確保に注力している。一方、インターネットを利用したビジネスの連携も急速に拡大している。たとえば、同業のメーカーが集合して部品調達の安定とコストダウンを図ったり、電子モールを形成してユーザによる選択の可能性を広げたりといった展開のほか、同一ブランドを利用する異業種連合も増えている。そうした場合、ASPには、それら同業または異業種の連合体がユーザから見たとき一体感をもつサービス設計が求められる。

【0004】

【発明が解決しようとする課題】しかしながら実際には、企業毎にサイトのドメイン名が異なり、連合体としての一体感をウェブ上に形成することに壁がある。本発明はこの点を認識した本発明者によってなされたものであり、ひとつの目的は、複数主体の連携に一体感をもたせたサービスをログインの管理という技術要素から実現することにある。本発明の別の目的は、ビジネスが拡大しつつあるASPの観点から、一体感のあるサービスを実現することにある。本発明のさらに別の目的は、ユーザを会員として扱うサービスにおいて、ユーザのログインを簡略化しつつセキュリティ面にも考慮した技術を提供することにある。

【0005】

【課題を解決するための手段】本発明のある態様は、ログイン管理方法に関する。この方法は、ユーザが認証のための情報を入力してネットワーク上の第1のサイトへ

ログインした後、そのサイトからリンクを辿って第2のサイトへのログインを試みたとき、第1のサイトにて前記認証のための情報を第2のサイトへアクセスするためのアドレスに付加して当該アクセスに提供するものである。

【0006】ここで「サイト」は、サイト内のサーバその他任意のノードでよく、ここでは総称的にサイトと呼ぶに過ぎない。アドレスの例はURL (Uniform Resource Locator) であり、例えばユーザが第1のサイトをウェブブラウザで閲覧しているとき、ページ上に設けられた第2のサイトへのリンクをクリックしたとする。このとき、ユーザのブラウザには第2のサイトのURLが設定される。本態様では、そのURLに認証のための情報（以下、単に認証情報ともよぶ）が付加される。例えばブラウザの機能によって認証情報とURL本体が分解され、第2のサイトへアクセスするとともに、第2のサイトから発せられる認証の要求に自動対応することができる。認証情報の例としてユーザIDとパスワードの組があるが、もちろんこれに限られない。認証情報はそのままの形でアドレスに付加される場合のほか、ワンタイム化され、または暗号化された後に付加されてもよく、そうした場合も含めて「第1のサイトにて前記認証のための情報を第2のサイトへアクセスするためのアドレスに付加して当該アクセスに提供する」と表現する。

【0007】この態様によれば、ユーザは第2のサイトへのログインの際に新たな認証手続を経る必要がない。したがって、例えば第1のサイトと第2のサイトが協力関係にある場合、ユーザの利便性を高め、かつサービスの一体感を醸成することができる。

【0008】認証情報の有効期限を第1のサイトから第2のサイトへ適宜設定し、第2のサイトは第1のサイトからリンクを辿ってログインするユーザのアクセスを前記有効期限内に限り許可してもよい。「第1のサイトから第2のサイトへ」とは、必ずしも第1のサイトが主体的である必要はなく、第2のサイトがいわゆるプル型の動作で設定内容を取得してもよい。この設定は、例えばアクセスを許すユーザの認証情報を列記したリストで通知されてもよく、その場合、そのリストに記載する認証情報を適宜変更して通知することにより、実用上まったく問題なく有効期限を設定することができる。例えば、30分間隔でリストを送信し、かつ、あるユーザの認証情報は1回に限りリストに載るようになれば、事実上そのユーザの有効期限が30分となる。ユーザごとにリストに載せる回数を変えれば、有効期限を変化させることもできる。なお当然ながら、ユーザの認証情報ごとに直接的に有効期限を記述して送信してもよい。

【0009】本発明の別の態様もログイン管理方法に関する。この方法は、ユーザが所定のサイトへのログインを試みたとき、そのユーザをそのサイトを代理する中継拠点へ導く工程と、その中継拠点にて得られたサイトの

情報をその中継拠点からユーザへ提供する工程とを含む。この構成にて、中継拠点がサイトの情報を得る際、そのサイトに認証のための情報を送信し、そのサイトからひとりのユーザとして認証された後、そのサイトへログインする。

【0010】本発明のさらに別の態様もログイン管理方法に関する。この方法は、ユーザが認証のための情報を入力してネットワーク上の第1のサイトへログインした後、そのサイトからリンクを辿って第2のサイトへのログインを試みたとき、そのユーザを第2のサイトの代理サーバへ導く工程と、その代理サーバにて得られた第2のサイトの情報をその代理サーバからユーザへ提供する工程とを含む。この構成において、代理サーバが第2のサイトの情報を得る際、第2のサイトからひとりのユーザとして認証された後、第2のサイトへログインする。

【0011】この態様であれば、代理サーバがユーザに代わって第2のサイトへログインするため、ユーザ自身は再度ログインのための手続をとる必要がない。一方、そのユーザは第1のサイトへのログインの際には認証されているため、セキュリティ面でのケアはなされている。

【0012】そのユーザがリンクを辿る際、第1のサイトはそのユーザが第2のサイトの情報を得ることができ有効期限に関する情報を代理サーバへアクセスするためのアドレスへ付加して当該アクセスへ供してもよい。また、有効期限に関する情報は暗号化されており、代理サーバはその情報を復号して解釈し、有効期限が切れたときそのユーザに対する第2のサイトの情報の提供を停止してもよい。

【0013】有効期限を設ける利点はセキュリティにある。上述の構成の場合、第2のサイトはユーザの認証を第1のサイトへ委任することができる。あるユーザが第1のサイトへログインしたときに限り第2のサイトへのリンクが見える構成とすれば、第2のサイトへのアクセスを事実上制限できる。しかし、このユーザが第2のサイトへアクセスしている間にこれをブックマークした場合、以降このユーザでない者であっても、このブックマークを頼りに第2のサイトへアクセスしうる。いま、第2のサイトが会員のみを開示されるべき情報を発信していれば、セキュリティ面で改善の余地がある。このため、有効期限を比較的短く設定すれば、たとえブックマークされても、このユーザ以外の者による第2のサイトの閲覧を阻止しやすくなる。

【0014】本発明のさらに別の態様は、ログイン管理システムに関する。このシステムは、第1のサイトを含む。第1のサイトは、ユーザが認証のための情報を入力してログインを求めたときユーザを認証する認証部と、ログインしたユーザに対して第2のサイトへのリンクを提供するリンク制御部とを含む。リンク制御部は、前記認証のための情報を付加した形で前記ユーザが第2のサ

イトへアクセスするためのアドレスを生成するアドレス生成部を含む。

【0015】本発明のさらに別の態様もログイン管理システムに関する。このシステムは、ユーザが所定のサイトへアクセスする際、そのアクセスを仲介する中継拠点を含む。この中継拠点は、前記サイトから、自身がユーザとして認証を受けるために必要な情報を送信する認証要求部と、前記サイトからユーザとして認証されたとき、このサイトへログインして取得した情報を前記ユーザへ提供する情報転送部とを含む。

【0016】本発明のさらに別の態様もログイン管理システムに関する。このシステムは、第1のサイトと代理サーバとを含む。第1のサイトは、ユーザが認証のための情報を入力してログインを求めたときユーザを認証する認証部と、ログインしたユーザに対して第2のサイトへのリンクを提供するリンク制御部とを含む。リンク制御部は、前記ユーザが前記代理サーバへアクセスするためのアドレスを生成するアドレス生成部を含む。また、代理サーバは、第2のサイトから、自身がユーザとして認証を受けるために必要な情報を送信する認証要求部と、第2のサイトからユーザとして認証されたとき、このサイトへログインして取得した情報を前記ユーザへ提供する情報転送部とを含む。

【0017】したがって、ユーザが第1のサイトへ認証を経てログインした後、第2のサイトへリンクを辿ってアクセスしようとしたとき、代理サーバへ接続される。代理サーバ自身はひとりのユーザとして第2のサイトから認証され、以降、そのサイトの情報をユーザへ提供する。

【0018】代理サーバはさらに、有効期限に関する情報を解釈してその期限の経過を監視する期限監視部を含み、その期限が経過したとき前記ユーザへの情報の提供が停止されてもよい。情報の提供の停止は、代理サーバがそのユーザのために第2のサイトと張ったセッションを切断してもよいし、情報転送部による転送を禁止してもよい。

【0019】本発明のさらに別の態様もログイン管理システムに関する。このシステムは、ユーザが最初にログインする第1のサイトと代理サーバとを含む。代理サーバは前記第1のサイトと類似のドメイン名のもとで構築される。類似は同一を含み、また第1のサイトのドメイン名のサブドメイン名などを含む。ユーザが第1のサイトとセッションを有する間に第2のサイトへのログインを要求したとき、第1のサイトはそのユーザのアクセス先を代理サーバへ変更する。代理サーバは、そのユーザに代わって第2のサイトから情報を取得してこれをそのユーザへ提供する。

【0020】なお、以上の構成要素の任意の組合せや組み替え、本発明を方法、システム、コンピュータプログラム、記録媒体などと表現したものもまた、本発明の態

様として有効である。

#### 【0021】

【発明の実施の形態】実施の形態1. 図1は、実施の形態1に係るログイン管理システム10の構成を示す。ログイン管理システム10において、ユーザ端末12、第1のサイトである会員管理サイト14、および第2のサイトである協力会社サイト30が明示しないインターネットで接続されている。会員管理サイト14のドメイン名はweb-a.com、協力会社サイト30のドメイン名はweb-b.comである。

【0022】会員管理サイト14は、あるサービスに関して協力会社サイト30と協力しており、そのサービスに関して会員を募集し、また会員に窓口として機能する。したがって、ログイン管理システム10には協力会社サイト30以外にも多数の協力会社が存在してもよく、その場合、窓口としての会員管理サイト14の意義が高まる。一例として、会員管理サイト14は会員に稀少商品を提供するバーチャルモールで、協力会社サイト30はそれに店出している輸入雑貨店である。会員には会費をもらう関係上、協力会社サイト30は会員のみにアクセスを認める。

【0023】会員管理サイト14は認証部16、リンク制御部18、および期限設定部22を有する。認証部16はユーザがログインを要求したとき(図中経路s)、これを認証する。ユーザがこのサービスの会員になると、ユーザIDとパスワード(以下、認証情報ともいう)が与えられる。なお、以下とくに断らない限り、「ユーザ」と「会員」を表現上区別しない。

【0024】認証されたユーザは会員管理サイト14の会員用ページへログインできる。このページには種々の情報があり、その中に協力会社サイト30へのリンクもある。このリンクは会員管理サイト14にログインできたユーザのみに見えるようページが構成されている。

【0025】リンク制御部18はユーザがそのリンク箇所をクリックしたときこのアクションを取得する。リンク制御部18のアドレス生成部20はユーザ端末12のブラウザに設定すべきアドレス、すなわち協力会社サイト30のURLを生成する。通常、そのURLは固定であるが、ここでは後述のようにそのユーザの認証情報をURLに付加したうえでブラウザへ設定する。ブラウザはURLに付加された認証情報を抽出し、本来のURL部分のみを協力会社サイト30へのアクセスへ利用するとともに、協力会社サイト30からユーザIDとパスワードの入力が求められたとき、前述の抽出した認証情報を協力会社サイト30へ自動的に送信する。この機能は最近標準的に利用されるウェブブラウザに実装される機能であり、本実施の形態ではそれを利用する。以上の処理の結果、ユーザのアクセス先は概念的に図中の経路tを辿り、ユーザ端末12の接続先が図中の経路uにしたがって協力会社サイト30となる。

【0026】期限設定部22は、ユーザが協力会社サイト30にアクセスできる有効期限を設定する。期限設定部22は協力会社サイト30の図示しない認証サーバに後述の「アクセス許可ユーザリスト」をFTP(File Transfer Protocol)で送信する。そのリストには、協力会社サイト30へのアクセスを認めるユーザの認証情報が記述されており、協力会社サイト30の認証サーバは、そのリストを見てユーザのアクセスを制限する。

【0027】図2はユーザがリンクを辿る際に生成されるURLを示す。まず、ユーザは最初に認証情報であるIDとパスワード(図中ID:PW)を入力して会員管理サイト14へのログインを試みる。認証部16は認証情報を取得してログインを認めるとともに、この情報をアドレス生成部20へ通知する。アドレス生成部20は認証情報を付加してURLを以下のように生成し、これがユーザ端末12のブラウザに設定される。

http://ID:PW@www.web-b.com/xxx

【0028】図3は前述のアクセス許可ユーザリスト32を示す。アクセス許可ユーザリスト32には協力会社サイト30へのアクセスを認めるユーザの認証情報がログインした順のシリアル番号によって記述されている。ここでは、ログイン番号33~50のユーザ、つまり認証情報として「ID33:PW33」~「ID50:PW50」のユーザのアクセスが許可されている。アクセス許可ユーザリスト32は期限設定部22から協力会社サイト30へ例えば1時間に1回送信され、次回送信の際、現在リストアップされている認証情報がクリアされ、「ID51:PW51」以降の認証情報が代わりに記述される。この方法により、ユーザのアクセスを1時間に限定することができる。なお、ここでは「アクセスを認めるための有効期限」といったが、これはログインできる有効期限やセッションの継続時間としての有効期限を含む。セッションの継続時間が1時間を超えたとき、協力会社サイト30の認証サーバその他の構成はその旨をユーザへ通知して再ログインを促してもよい。

【0029】図4は以上の構成によるサービスの一例を示す。会員用画面40は、ユーザが最初に会員管理サイト14の認証を受けてログインしたときに現れる。ここでは、会員管理サイト14によるサービスが「○○○オンラインモール」と表示され、このユーザが「会員△△△」と表され、会員には割引の特典がある旨が示されている。画面下部には「商品ディレクトリ」のタイトルのもと、「日用品」「家具」「衣料品」などが列挙されている。ここでユーザが衣料品のリンク42をクリックすると、リンク制御部18でそのアクションが取得され、以降上述の処理を経て「衣料品」を担当する協力会社サイト30へのアクセスが実現する。

【0030】以上、本実施の形態によれば、ユーザは会員管理サイト14へログインすれば協力会社サイト30へのログインに際して再度認証手続を行う必要がない。

このため、ユーザの利便性が高まると同時に、会員管理サイト14と協力会社サイト30の連携によるサービスに一体感が出る。また、協力会社サイト30も実際には会員管理サイト14からの認証情報を用いた認証をしているため、セキュリティも配慮されている。さらに、アクセスに有効期限を設けたため、協力会社サイト30のURLがブックマークされた場合でも、会員以外の者は容易にアクセスができない機構が実現する。

【0031】なお、図2では理解の簡単のために、ユーザが入力した認証情報である「ID:PW」がそのままアドレス生成部20によって生成されるURLに組み込まれる形で説明したが、現実には両者は異なることが、セキュリティ上もアドレス生成アルゴリズムの単純化の上でも望ましい。このために、アドレス生成部20によって生成されるURLに組み込まれる「ID:PW」にワンタイム性をもたせればよく、一例として単純にシリアル番号を付与すればよい。その場合、図3のアクセス許可ユーザリスト32の内容も単純にシリアル番号の記載で済み、管理上もリスト作成上もメリットがある。ただし、よりセキュリティを高める観点からいえば、当然ワンタイム化に際してランダム化等の処理を加えることが望ましい。

【0032】実施の形態2. 図5は実施の形態2に係るログイン管理システム100の構成を示す。実施の形態1と異なり、代理サーバ110が設けられ、ユーザの協力会社サイト30へのアクセスが代理サーバ110を通じて行われる。実施の形態2では、代理サーバ110を会員管理サイト14と類似のドメイン名を利用して構築\*

<http://ztAjJ4kiq1SI.web-a.abc-proxy.com> (式1)

【0035】ユーザは会員管理サイト14にログインし(経路s)、会員専用のページで協力会社サイト30へのリンクを見つけ、これをクリックする。アドレス生成部20はそのURLに有効期限を付加してブラウザへ設定する。これでユーザのアクセス先が代理サーバ110になる(経路u)。代理サーバ110はCGI(Common Gateway Interface)などによりユーザからアクセスがあったとき、協力会社サイト30から情報を取得してユーザへ転送するよう動作する。代理サーバ110はユーザに代わって協力会社サイト30へログインし(経路v)、協力会社サイト30の情報をユーザへ閲覧させる(経路v、w)。これにより、実質的にアクセス先が会員管理サイト14から協力会社サイト30へ移動する(経路t)。

【0036】代理サーバ110は期限監視部112、認証要求部114、および情報転送部116を有する。認証要求部114は、ユーザがアクセスしてきたとき、協力会社サイト30へログインするためにユーザIDとパスワードを送信して認証手を要求する。このユーザIDとパスワードはユーザのものではなく、代理サーバ110自身のもので、協力会社サイト30から代理サーバ

\*でき、さらにサービスの一体感が高まる。

【0033】ユーザから協力会社サイト30へのリンクは、実施の形態1同様、会員管理サイト14へログインできた会員のみから見え、また協力会社サイト30へのアクセスが代理サーバ110で中継される。そのため協力会社サイト30のセキュリティは高い。代理サーバ110はユーザの代わりに協力会社サイト30の情報を取得するため、協力会社サイト30から見ればひとりのユーザとして認証を受ける。いわゆる代理サーバが、その代理するサイトとの間でID、パスワードなどによる認証手続を経る点に特徴的である。以下、実施の形態1同様の構成には同じ符号を与え、実施の形態1との差を中心に説明する。

【0034】期限設定部22はアドレス生成部20内部へ移動し、アドレス生成部20はさらに暗号化部102を有する。この実施の形態では、暗号化部102で生成された有効期限は、暗号化部102で暗号化された後、URLに付加される。ただし、そのURLは協力会社サイト30ではなく代理サーバ110を指している。有効期限はリストに記述されるのではなく、アクセスの「開始時刻」と「終了時刻」などの形で直接的に記述される。DNS(Domain Name Server)にはその標準的な機能としてワイルドカード指定が可能なものがあり、この実施の形態では、ワイルドカードの部分に有効期限を書き込む。アドレス生成部20で生成されるURLの一例は以下のとおりであり、この暗号化された「ztAjJ4kiq1SI」の部分を実際のワイルドカード指定してDNSを通す。

110はひとりのユーザに見える。代理サーバ110が協力会社サイト30へログインした後、情報転送部116は協力会社サイト30の情報をユーザへ転送する。

【0037】期限監視部112は、アドレス生成部20がURLに埋め込んだ有効期限を検出して復号し、期限の到来を監視する。期限が到来したとき、代理サーバ110と協力会社サイト30のセッションを切断する。

【0038】図6は、ユーザが代理サーバ110へアクセスするまでの処理を示す。ユーザはまず、会員として最初に会員管理サイト14へアクセスし、認証部16による認証を受け(S10)、会員管理サイト14へログインする(S12)。ユーザはつぎに協力会社サイト30へのリンク箇所をクリックする(S14)。アドレス生成部20は式1に示すURLを生成し(S16)、これがユーザ端末12のブラウザに設定され、代理サーバ110へのアクセスが実現する(S18)。

【0039】図7は代理サーバ110からユーザ端末12に情報が提供される処理を示す。ユーザからアクセスされたとき、またはそれ以前の任意のタイミングにおいて、協力会社サイト30は認証要求部114からのログイン要求に応じてこれを認証する(S30)。認証後、

代理サーバ110は協力会社サイト30へログインする(S32)。ユーザが代理サーバ110へアクセスしたとき、そのユーザに関する有効期限が到来していなければ(S34のN)、情報転送部116がユーザのアクションを取得して(S36)必要なページを協力会社サイト30からユーザ端末12へ転送する(S38)。この後、有効期限が到来するまで同様の処理を繰り返し、期限が来たら(S34のY)、そのユーザのためのセッションを切断し(S40)、処理を抜ける。

【0040】以上、本実施の形態によれば、ユーザが仮に協力会社サイト30をブックマークしようとしても代理サーバ110のURLしかわからず、そのURLも有効期限で無意味になるので、会員でないユーザがこのユーザ端末12を利用しても協力会社サイト30の情報が得られない。有効期限は暗号化されているため、これをもとに有効期限を操作することもきわめて困難である。有効期限を開始時刻や終了時刻のように刻々変化する情報で表現するため、暗号化された情報のワンタイム性も高く、さらにセキュアである。

【0041】以上、本発明を実施の形態をもとに説明した。この実施の形態は例示であり、それらの各構成要素や各処理プロセスの組合せにいろいろな変形例が可能なこと、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。

【0042】例えば、図4では電子モールを例示した。しかし、本発明はそれ以外にも種々のサービスに利用可能である。一例として協力会社サイト30に機密性のある情報を配し、会員管理サイト14で閲覧者を管理する。例えば、協力会社サイト30が製薬会社の場合、劇薬その他のデータの閲覧に医師の資格が必要である。協

10

20

30

力が機密情報を含む各種情報を医師に提供する場合、会員管理サイト14はアクセスしてきたユーザが医師であるかどうかを確認した後、サービスを提供する。

【0043】

【発明の効果】本発明によればログインに際してユーザの利便性が高まる。または、本発明によればサービスの一体感が高まる。

【図面の簡単な説明】

【図1】 実施の形態1に係るログイン管理システムの構成図である。

【図2】 実施の形態1において、アドレスが生成される様子を示す図である。

【図3】 実施の形態1で利用されるアクセス許可リストの構成図である。

【図4】 実施の形態1の会員管理サイトにアクセスしたときに表示される画面を示す図である。

【図5】 実施の形態2に係るログイン管理システムの構成図である。

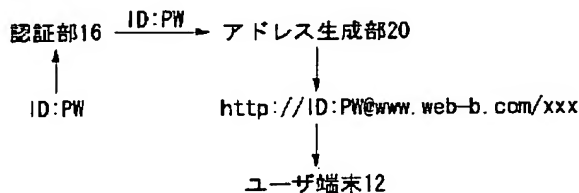
【図6】 実施の形態2において、アクセス先が代理サーバへ移行するまでの処理を示すフローチャートである。

【図7】 実施の形態2において、代理サーバからユーザ端末へ情報が提供される処理を示すフローチャートである。

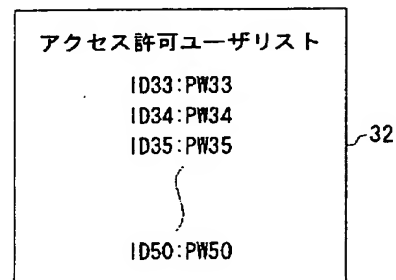
【符号の説明】

10、100 ログイン管理システム、 12 ユーザ端末、 14 会員管理サイト、 16 認証部、 18 リンク制御部、 20 アドレス生成部、 22 期限設定部、 30 協力会社サイト、 102 暗号化部、 110代理サーバ、 112 期限監視部、 116 情報転送部。

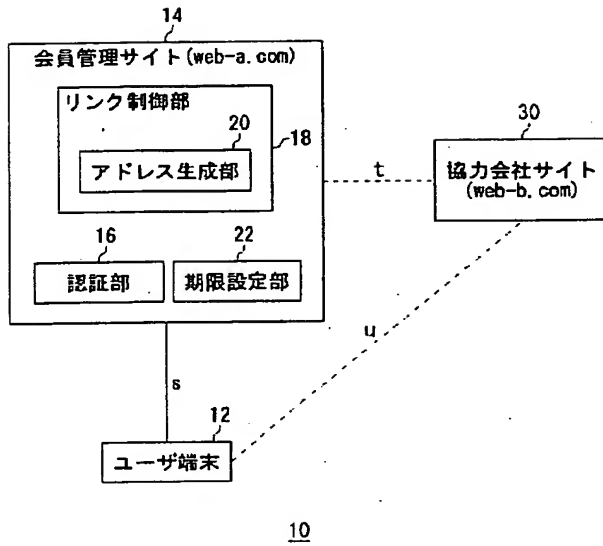
【図2】



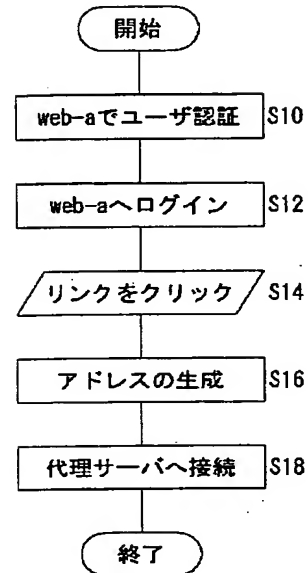
【図3】



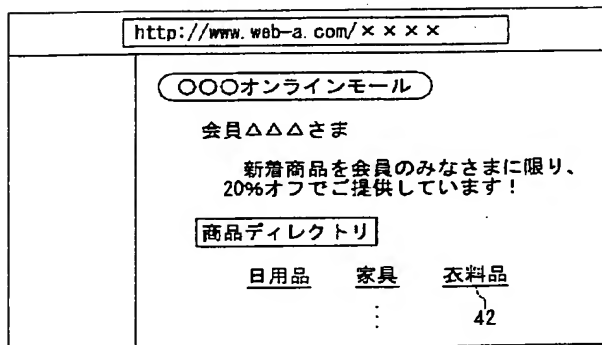
【図1】



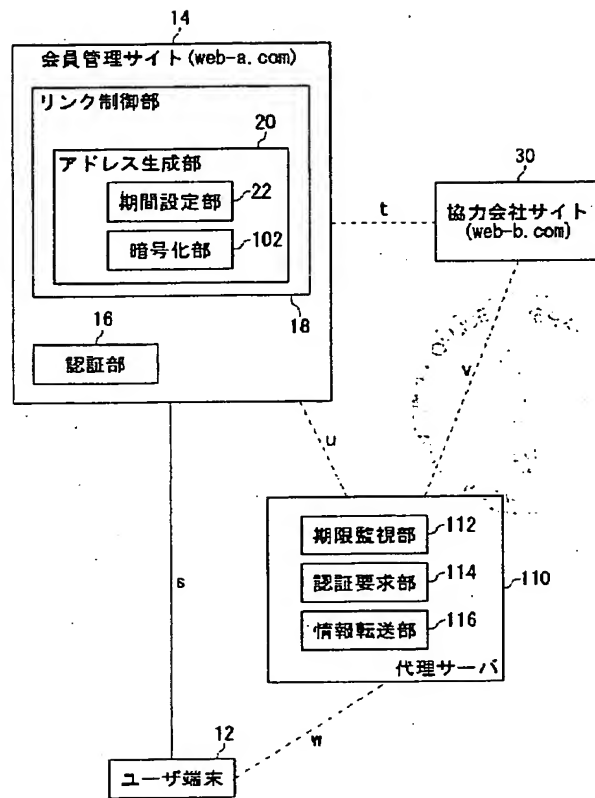
【図6】



【図4】



【図5】



100

【図7】

